Android Malware Hunting Cheat Sheet

Field-ready reference • Modern Android (10+) • Non-root & Root paths

QUICK TRIAGE START HERE

```
$ adb shell pm list
packages -f | sort
```

```
$ adb shell cmd
package list packages
--show-versioncode
```

```
$ adb shell appops
query-op --user 0
RUN_IN_BACKGROUND
```

```
$ adb shell dumpsys
package > /sdcard/
pkg.txt
```

```
$ adb shell settings
list secure | grep -i
debug
```

```
$ adb shell logcat -v
time -d | grep -iE
\"dex2oat|zygote|
frida|magisk\"
```

```
$ adb shell ps -A |
grep -iE \"frida|
magisk|xposed\"
```

```
$ adb shell ls -la /
data/local/tmp/
```

```
$ adb shell dumpsys
activity processes |
grep -i suspicious
```

```
$ adb shell ip addr ;
adb shell ip route
```

SUSPICIOUS APP LOCATIONS

/data/app/[package]-*/ – Installed APKs/odex

/data/data/[package]/ – App sandbox (db/prefs/files)

/data/user/0/[package]/ – Primary user app data

/storage/emulated/0/Android/data/[package]/ – Ext. app data

/system/priv-app/ – System-priv APKs (rogue?)

PERSISTENCE & AUTOSTART

/data/system/packages.xml – Installs/permissions

/data/system/package-usage.list – Last-used apps

/data/system/package-restrictions.xml – Enabled/disabled states

/system/etc/init.d/ – Legacy boot scripts

/data/adb/modules/ – Magisk modules

```
$ adb shell cmd package query-permission
android.permission.RECEIVE_BOOT_COMPLETED
```

ROOT • HOOKING • TAMPERING

/system/xbin/su , **/system/bin/su** – Root binaries

/data/adb/magisk/ – Magisk artifacts

/data/local/tmp/frida-server – Frida hook

/data/data/de.robv.android.xposed.installer/ – Xposed

/system/framework/ – Injected jars?

```
$ adb shell ls -la /system/xbin /system/bin |
grep -i su
```

C2 • CONFIG • PAYLOADS

/data/data/[pkg]/shared_prefs/ – XML configs, endpoints

/data/data/[pkg]/files/ – Dropped payloads

/data/data/[pkg]/databases/ – Tokens/URLs

/data/local/tmp/ – Staging area

/system/etc/hosts – DNS hijack

```
$ adb shell grep -RinE \"http(s)?://|wss://|
mqtt\" /data/data/[pkg]/
```

NETWORK & EXFIL

/proc/net/tcp , **/proc/net/udp** – Sockets

/proc/net/unix – Local sockets (IPC)

/data/system/netstats/ – Per-app usage

/data/misc/net/ – Net cfg/state

/data/misc/wifi/WifiConfigStore*.xml – Known SSIDs

```
$ adb shell logcat -d | grep -iE \"ssl|tls|
cert|socket|http\"
```

USAGE • TELEMETRY • APPOPS

/data/system/usagestats/ – FG/BG app events

/data/system/appops.xml – Permission ops

/data/system/uiderrors.txt – UID error traces

/data/system/notification_policy.xml – Notification policy

```
$ adb shell appops get [package] RUN_IN_BACKGROUND
```

LOGS • CRASH • BOOT

/data/system/dropbox/ – System events

/data/anr/traces.txt – ANR traces

/data/tombstones/ – Native crashes

/sys/fs/pstore/ – Persistent crash

/data/misc/bootstat/ – Boot/reset stats

```
$ adb shell logcat -b events -d | grep -i crash
```

CREDENTIAL & ACCOUNT SURFACES

/data/system/locksettings.db – Lock creds (hashed)

/data/system_ce/0/accounts_ce.db – Accounts/tokens

/data/misc/keystore/ – Keystore blobs

/data/system/sync/accounts.xml – Sync config

```
$ adb shell dumpsys account
```

HIDDEN • TEMP • MEDIA ABUSE

/data/local/tmp/ – Temp payloads

/storage/emulated/0/Download/.*/ – Hidden dirs

/storage/emulated/0/.nomedia – Scanner evasion

/storage/emulated/0/Android/data/[pkg]/cache/ – Droppings

```
$ adb shell find /storage/emulated/0 -type d -name \".*\" -maxdepth 3
```

BROWSER • WEB ARTIFACTS

/data/data/com.android.chrome/app_chrome/Default/History – History

/data/data/com.android.chrome/app_chrome/Default/Cookies – Cookies

/data/data/org.mozilla.firefox/files/mozilla/ – Profiles

/data/data/com.android.browser/databases/browser2.db – Legacy

```
$ adb shell strings /data/data/com.android.chrome/app_chrome/Default/Preferences | grep -i url
```

RUNTIME • PROCESS FORENSICS

/proc/[pid]/maps – Mappings

/proc/[pid]/fd/ – Open files

/proc/[pid]/cmdline – Launch args

/proc/[pid]/environ – Env vars

```
$ adb shell for p in $(pidof -s [package]); do cat /proc/$p/cmdline; done
```

SIGNALING • TELEPHONY

/data/user_de/0/com.android.providers.telephony/databases/mmssms.db – SMS/MMS

/data/user_de/0/com.android.providers.telephony/databases/telephony.db – SIM / carriers

/data/user_de/0/com.android.providers.contacts/databases/calllog.db – Calls

```
$ adb shell content query --uri content://sms --limit 5
```

TRIAGE QUERIES (NON-ROOT)

List pkgs	`$ adb shell pm list packages -f`
App info	`$ adb shell dumpsys package com.target.app`
Running	`$ adb shell dumpsys activity processes`
Net	`$ adb shell ip addr ; adb shell ip route`
Logs	`$ adb logcat -d | tail -n 200`

TRIAGE QUERIES (ROOTED)

UID map	`# grep -R \"u0_a\" /data/system/packages.list`
Find ELF	`# find /data -type f -perm -111 -exec file {} \\; | grep ELF`
Open net	`# cat /proc/net/tcp /proc/net/udp`
Recent	`# ls -lt /data/local/tmp | head`
Strings	`# strings /data/data/[pkg]/lib/* 2>/dev/null | grep -i \"http\\\|key\\\|token\"`